

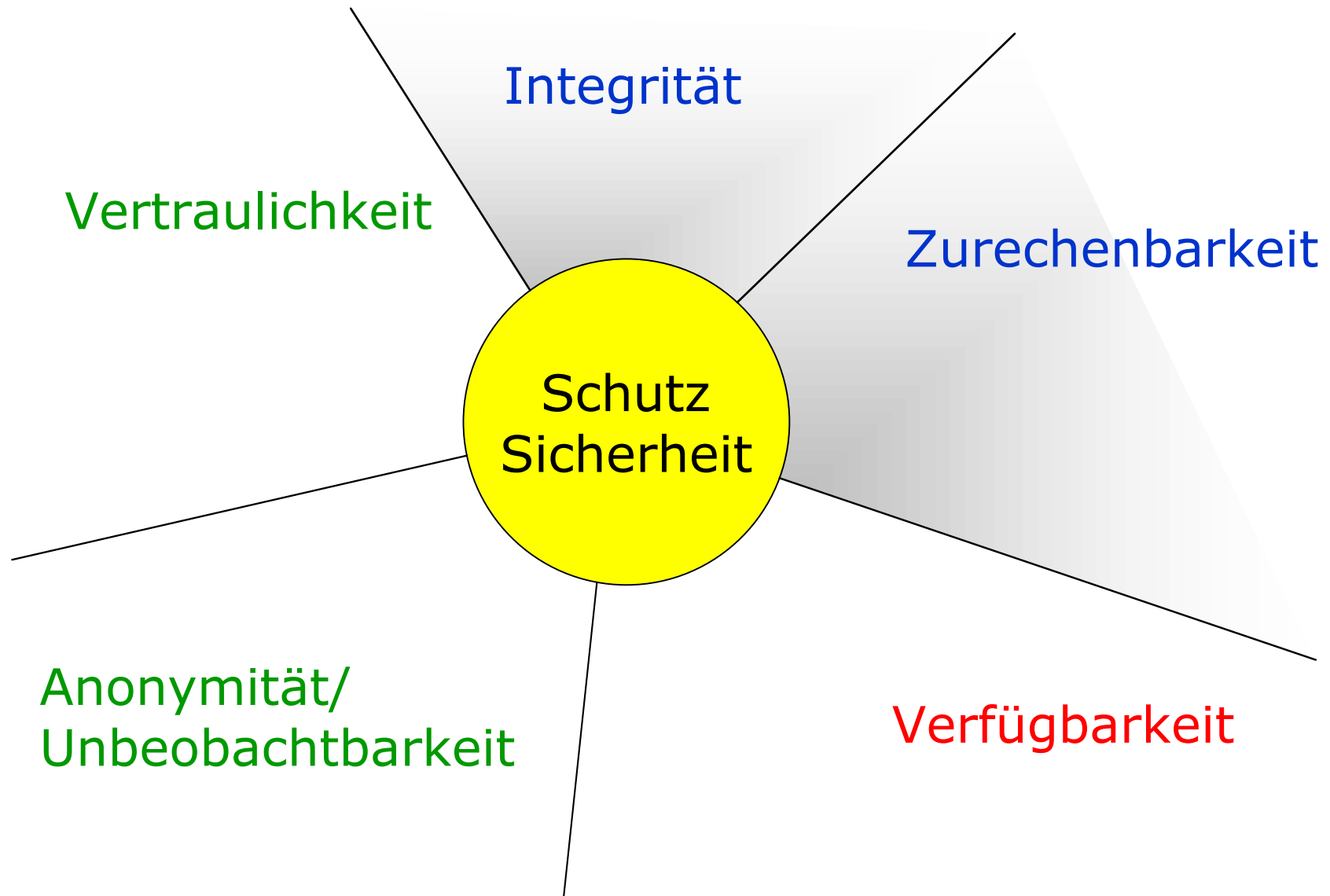
> Multimediale Inhalte und technischer Urheberrechtsschutz

Hannes Federrath

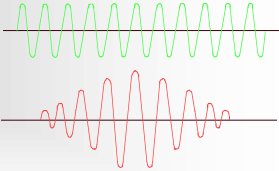
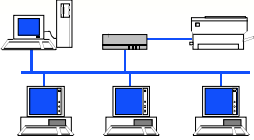

<http://www.inf.tu-dresden.de/~hf2/>

- ⌘ Distribution von MM-Inhalten im Internet
- ⌘ Techniken zum Schutz von Urheberrechten
- ⌘ Adressierung von Inhalten
- ⌘ Filterung illegaler Inhalte
- ⌘ Zusammenfassung

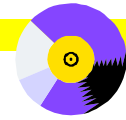
Schutz und Sicherheit



> Distribution von MM-Inhalten

| | ONLINE | OFFLINE |
|-----------|--|--|
| SYNCHRON | Rundfunk, Fernsehen  | — |
| ASYNCHRON | <p>z.B. on-demand Streaming services im Internet</p>  <p>Fähigkeit zur Interaktivität</p> | <p>z.B. Distribution über Datenträger</p>  |

> Klassische Distribution: Offline Medien

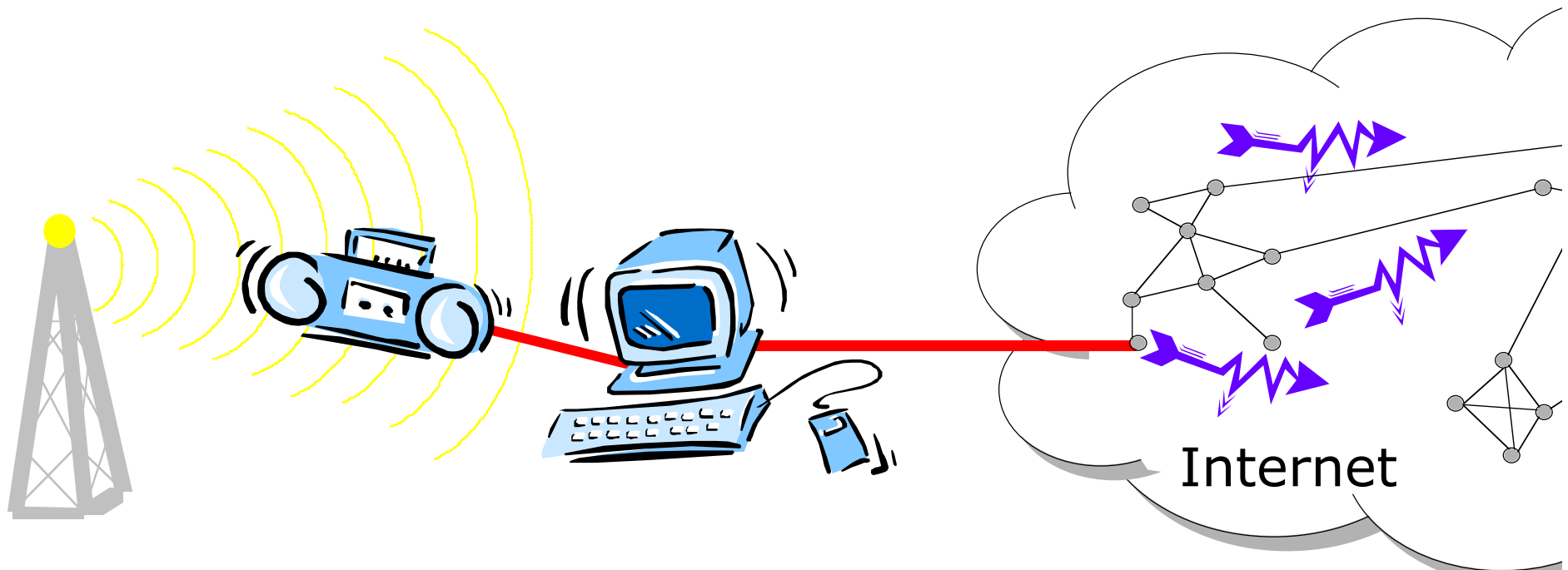


- ⌘ alle Kopien sind gleich
- ⌘ Herstellen von Kopien war bisher aufwendig/teuer
- ⌘ Schutzmöglichkeiten/Ansätze:
 - ⊗ Datenträger verschlüsseln und über ausforschungssichere Hardware entschlüsseln
 - ⊗ „Dongle“
 - ⊗ Ausgabe in niederwertiger Qualität
- ⌘ Probleme:
 - ⊗ Codes können geknackt werden
 - ⊗ zu teuer und begrenzte Sicherheit

Schutz nur gegen Gelegenheitstäter

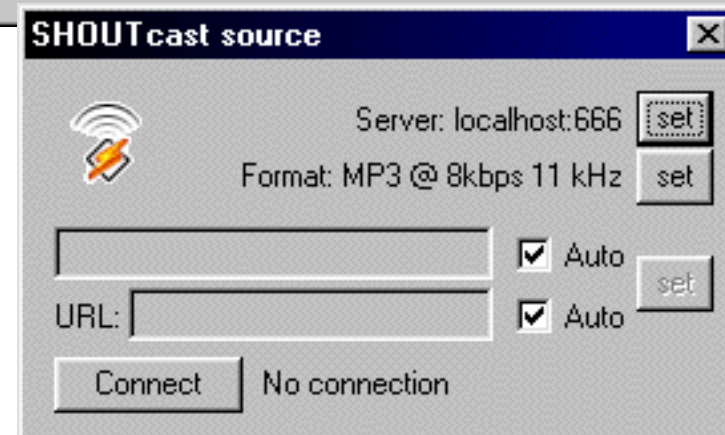
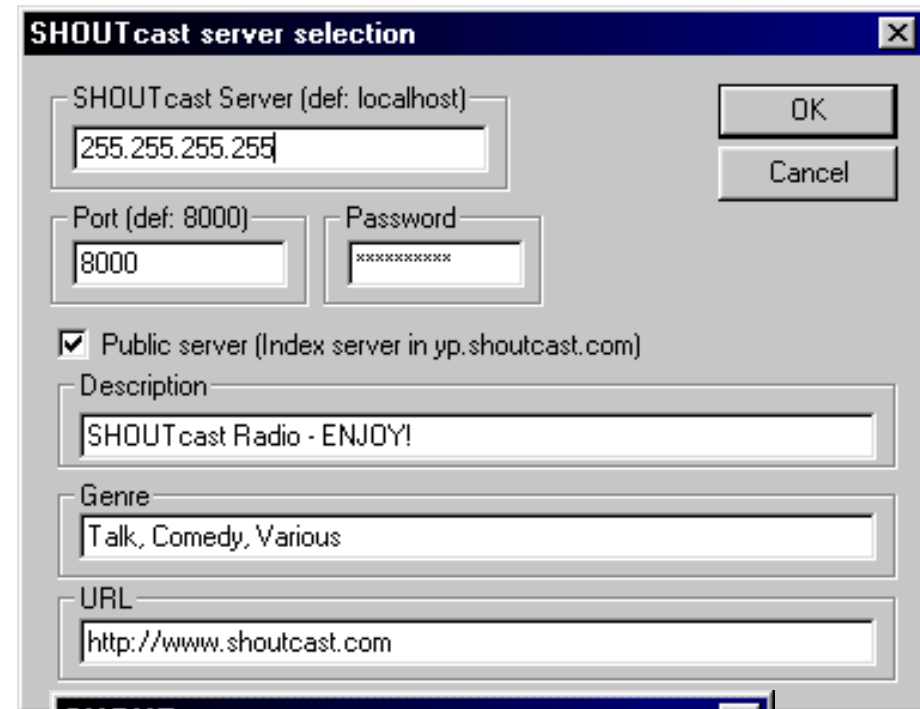
> Klassische Distribution: Rundfunk

- ⌘ alle Kopien sind gleich
- ⌘ Re-Distribution scheitert meist noch an technischen Möglichkeiten
- ⌘ Broadcast-Software für Jedermann:
 - ☒ SHOUTCast <http://www.shoutcast.com/>
- ⌘ live und on-demand MP3 Internet Broadcast



> Klassische Distribution: Online Medien

- ⌘ alle Kopien sind gleich
- ⌘ Re-Distribution scheitert meist noch an technischen Möglichkeiten
- ⌘ Broadcast-Software für Jedermann:
 - ☒ SHOUTCast
<http://www.shoutcast.com/>
- ⌘ live und on-demand MP3 Internet Broadcast



> Distribution im Internet

⌘ Heute: alle Kopien sind gleich

⌘ Herstellen von Kopien und Redistribution leicht

⊠ private Webpages

⊠ Newsgroups

⊠ Scour <http://www.scour.com/>

⊠ Napster <http://www.napster.com/>

⊠ Gnutella <http://gnutella.wego.com/>

⌘ Verfolgung meist möglich, aber aufwendig

⌘ Anonymitätsverfahren könnten Verfolgung verhindern:

⊠ Freenet <http://freenet.sourceforge.net/>

⊠ Freedom <http://www.freedom.net/>

⊠ Anon/WebMixe <http://anon.inf.tu-dresden.de/~hf2/anon/>

> Übertragungsprotokolle im Internet

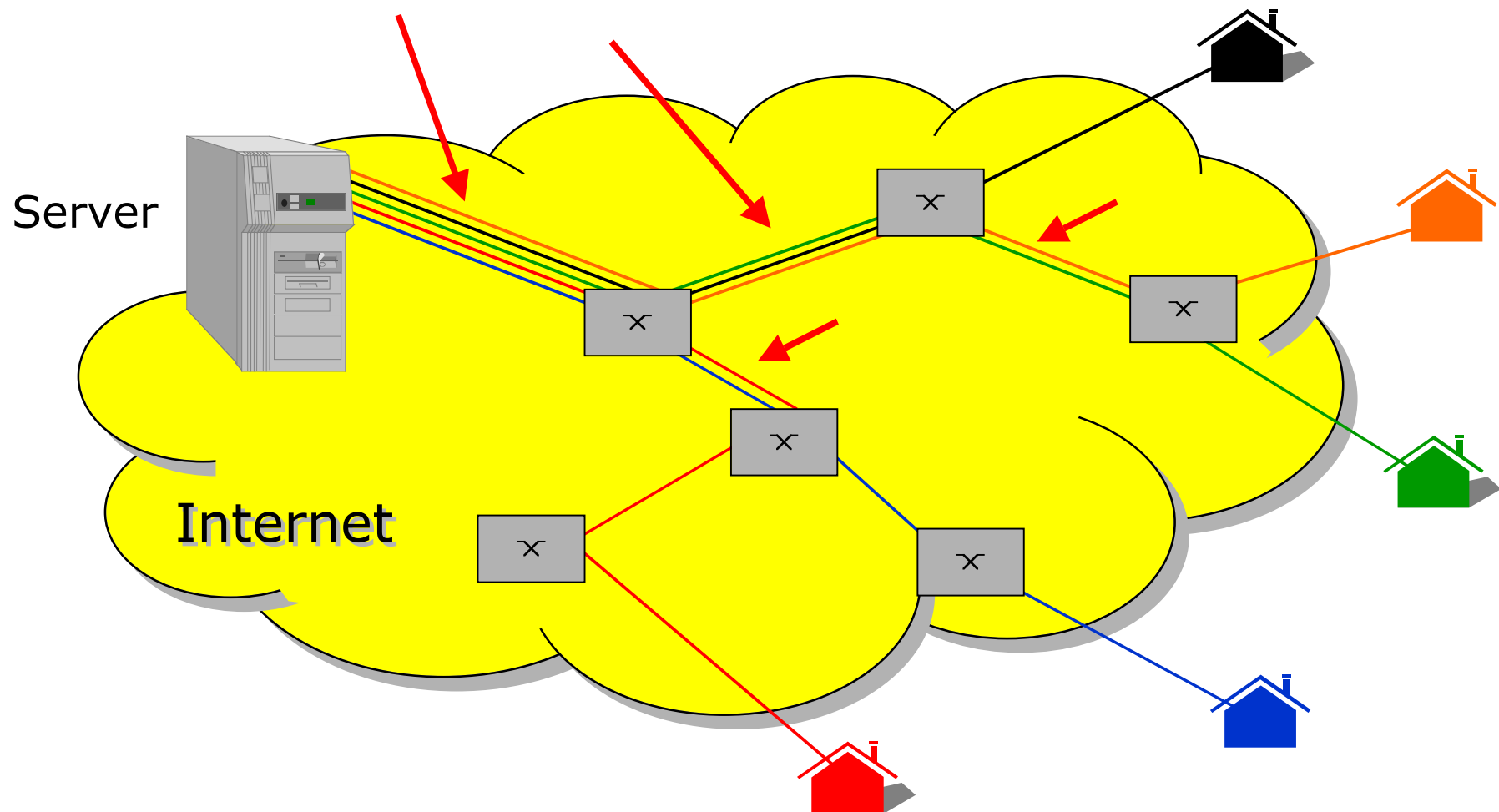
| | TCP | UDP |
|-------------------------|--------------------------------------|--|
| peer-to-peer | <i>etabliert</i> ✓ HTTP (WWW) | <i>etabliert</i> ✓ tlw. keine QoS-Zusicherungen Real |
| multicast/ broadcast | | <i>in Entwicklung und Erprobung</i> QoS: Quality of Service |

Transmission Control Protocol
gesicherte "Verbindung"
Retransmission

User Datagram Protocol
einzelne "Pakete"
Dropping

> Peer-to-peer

- ⌘ 1 Verbindung pro Client und Request
- ⌘ Unnötige Bandbreiteverschwendung

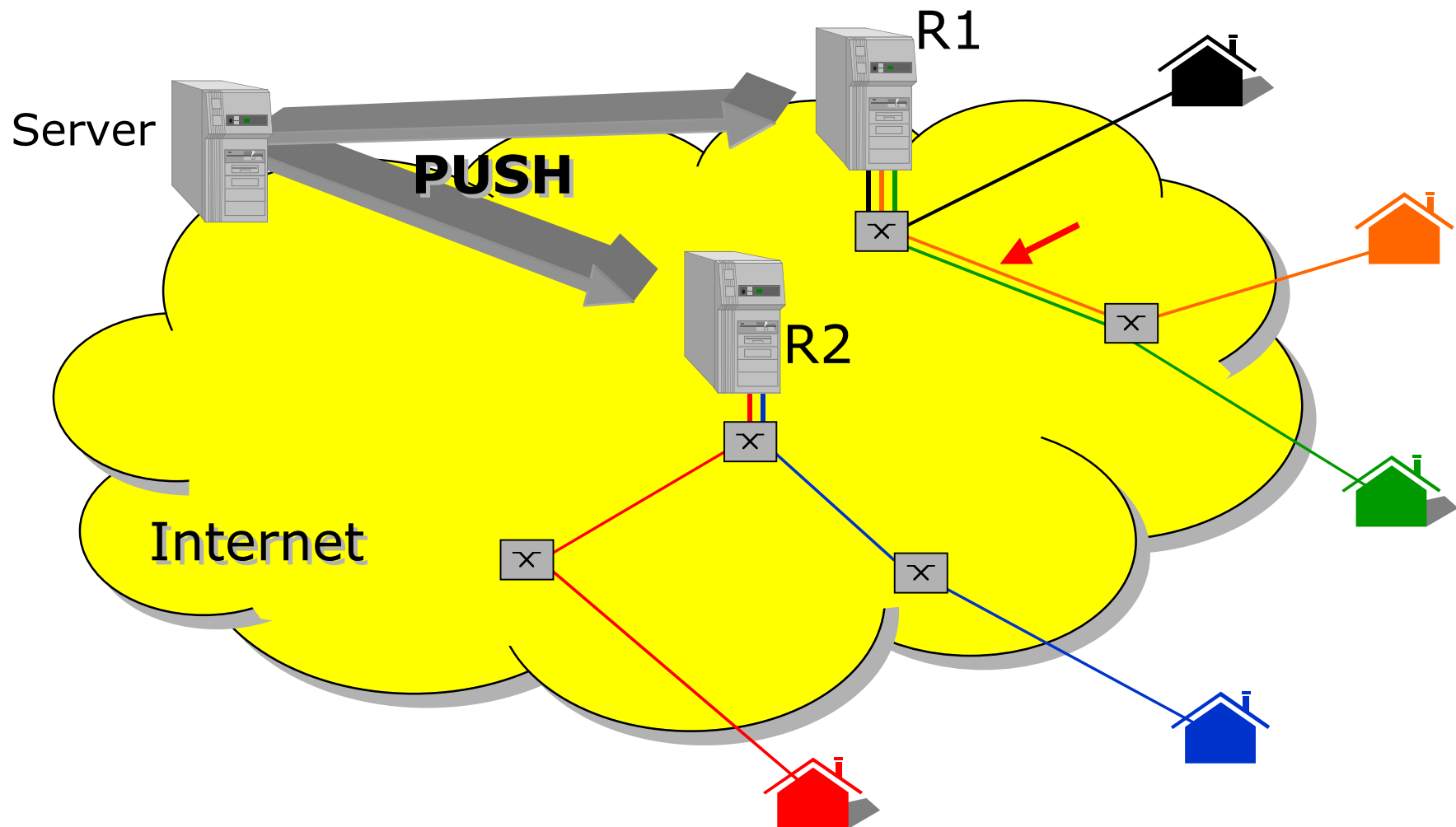


> Replikation des Datenbestandes

⌘ Replikation des Datenbestandes zur Lastverteilung

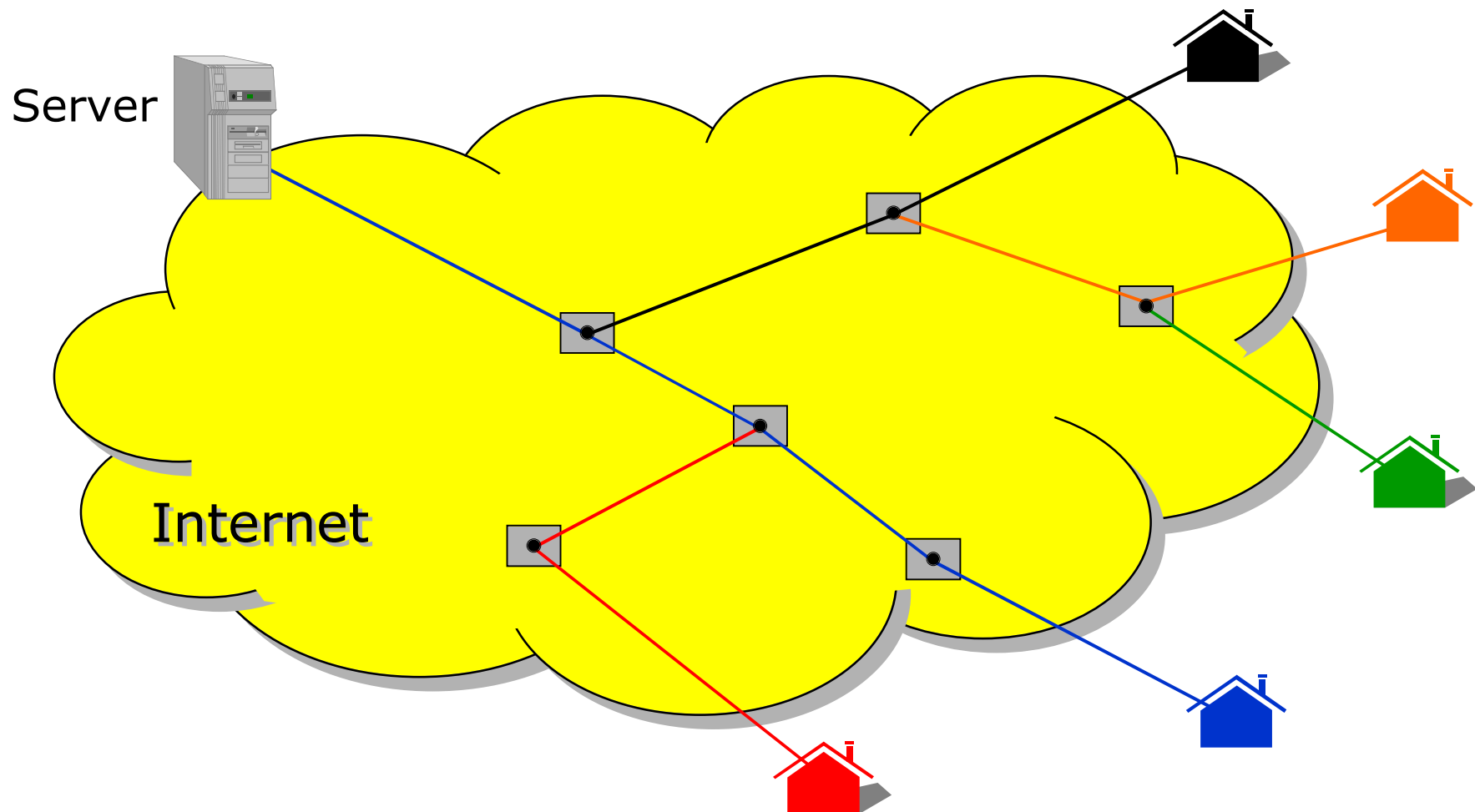
⌘ Akamai

<http://www.akamai.com>



> Multicast

- ⌘ „Anfordern“ z.B. eines streams
- ⌘ Quality of Service (QoS)



> Techniken zum Schutz

⌘ Watermarking:

- ⊗ Geschützte digitale Mediendaten markieren, damit sie als solche erkennbar sind und Manipulation erkennbar bleiben

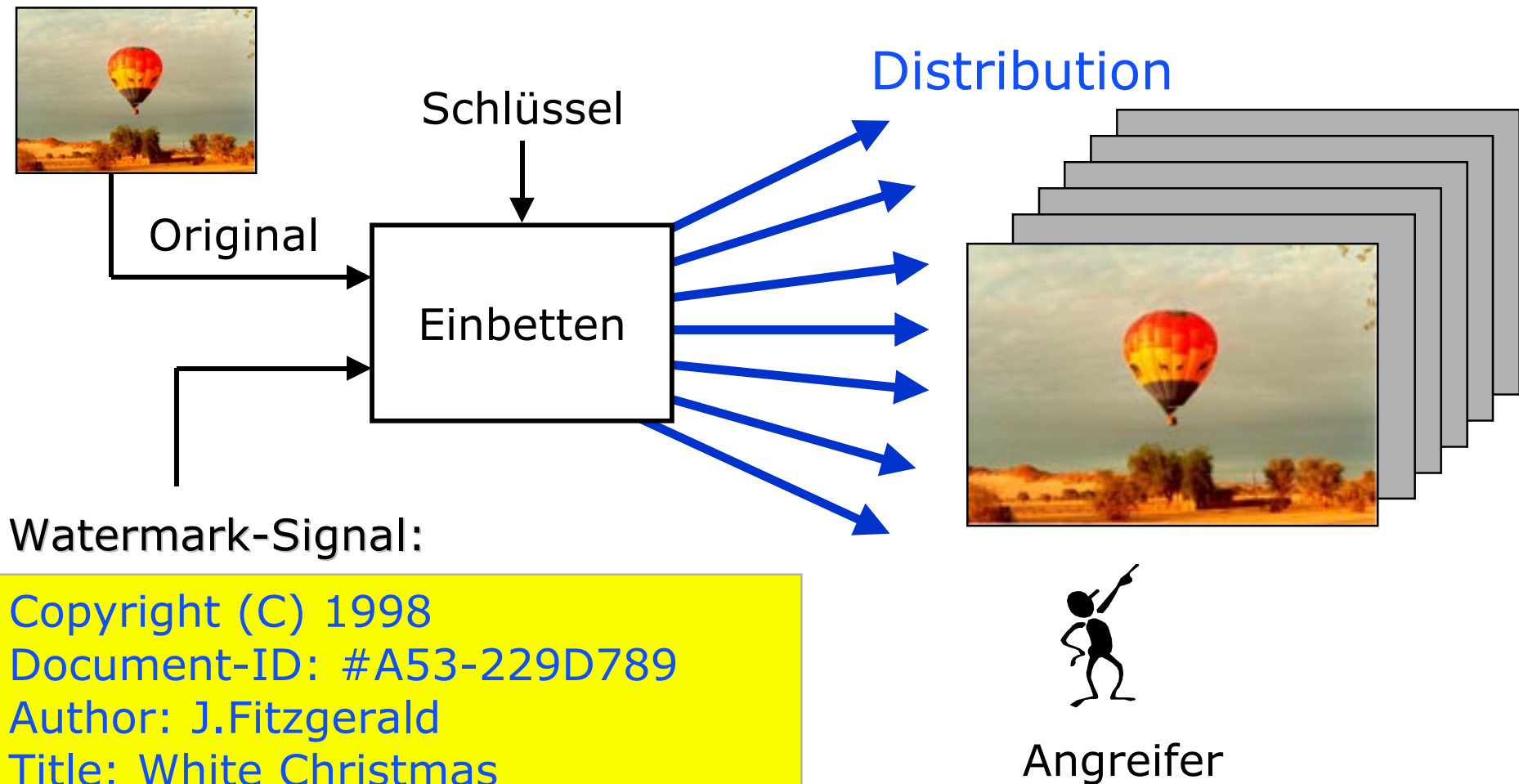
⌘ Encryption:

- ⊗ Individualisierte und kostenpflichtige Dienste vor unberechtigter Nutzung schützen

⌘ Traitor Tracing:

- ⊗ Individualisierung des legal erworbenen Inhaltes bzw. Entschlüsselungsschlüssels ermöglicht Rückverfolgung des illegalen Distributionsweges

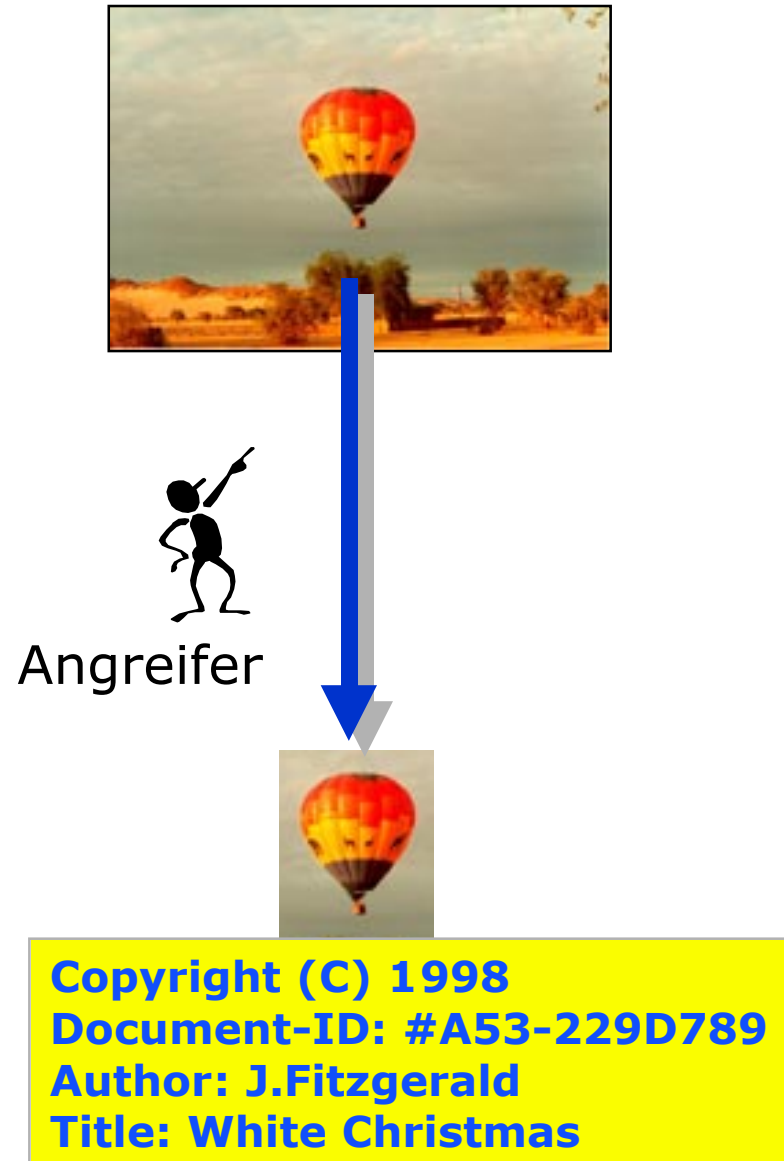
> Watermarking



> Watermarking

- ⌘ Digital-Analog-Wandlung
- ⌘ Analog-Digital-Wandlung
- ⌘ Re-Sampling
- ⌘ Re-Quantisierung
- ⌘ Kompression
- ⌘ Dithering
- ⌘ Rotation
- ⌘ Translation
- ⌘ Cropping
- ⌘ Scaling

- ⌘ Collusion Attacks



> Watermarking

⌘ Theorie

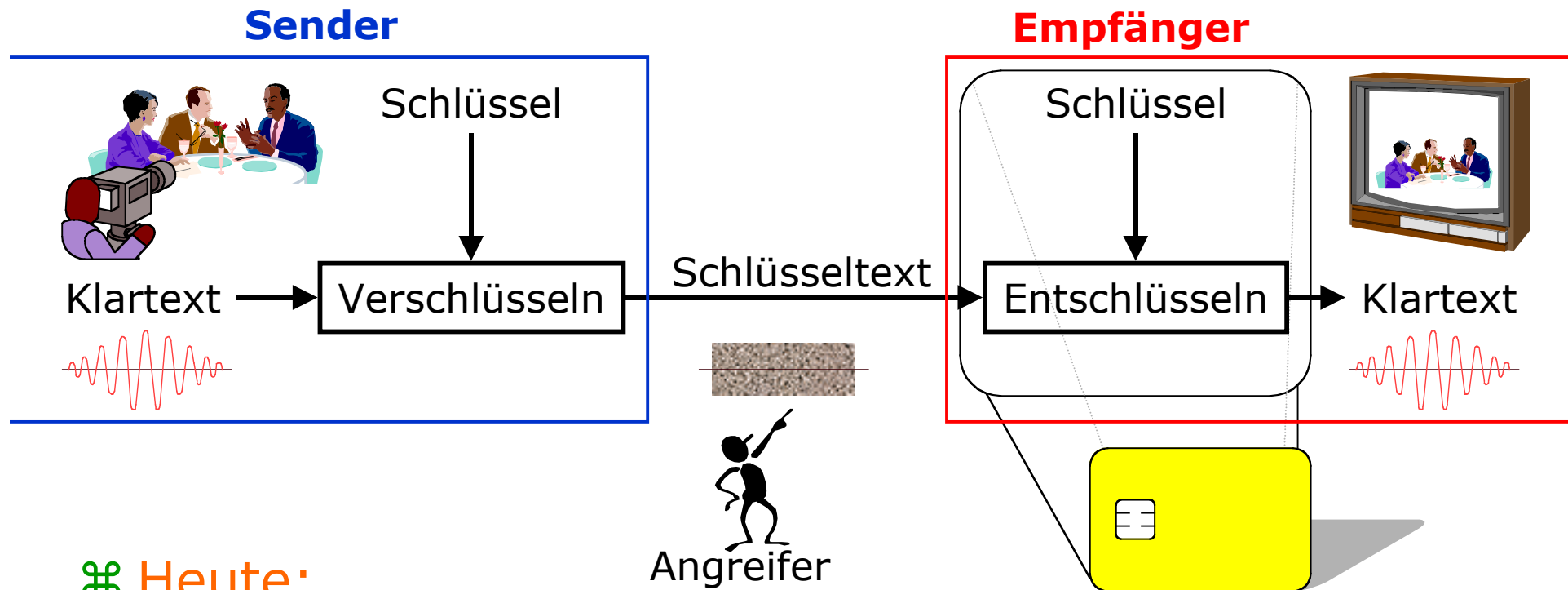
- ⊠ Robustheit
- ⊠ Beeinträchtigungslosigkeit
- ⊠ Nachweisbarkeit (Offenlegung des Schlüssels)

⌘ Praxis

- ⊠ **StirMark** (M. Kuhn, F. Petitcolas, 1997)
 - ⊕ automatisiertes Programm
 - ⊕ entfernt Watermark (WM)
 - ⊕ WM nicht mehr erkennbar durch Algorithmus
 - ⊕ <http://www.cl.cam.ac.uk/~fapp2/watermarking/stirmark/>

> Encryption

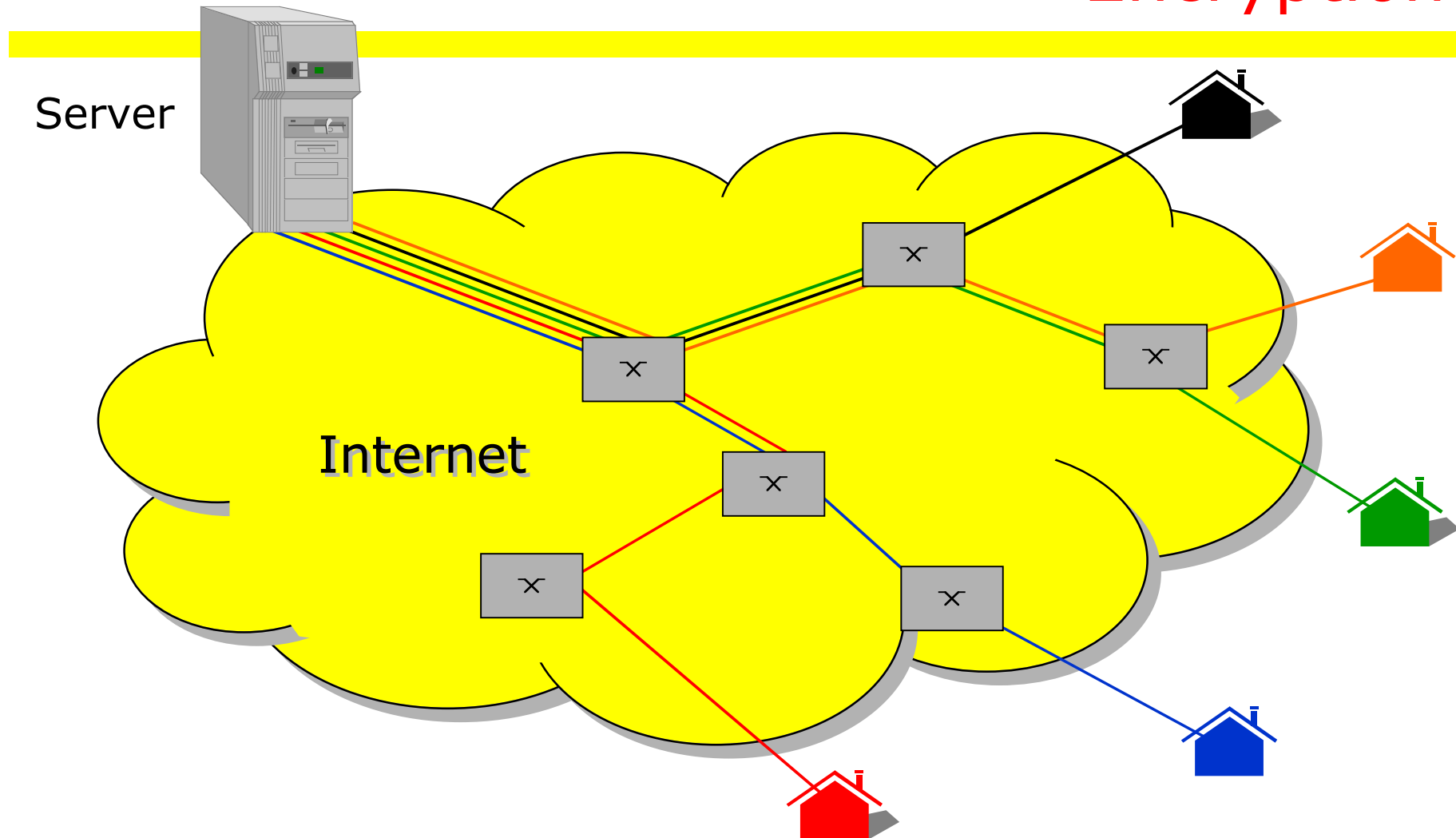
⌘ Individualisierte und kostenpflichtige Dienste vor unberechtigter Nutzung schützen



⌘ Heute:

- ⊗ entweder: tamper-resistant Hardware
- ⊗ oder: jeder Teilnehmer erhält individuell verschlüsselten stream

> Encryption



⌘ Internet: Jeder Teilnehmer erhält individuell verschlüsselten stream

> LoFi Broadcast, HiFi Encryption

⌘ Medienstrom aufteilen

- ⊠ Ein Teil wird an alle als exakte Kopie verteilt.
- ⊠ Ein Teil wird individualisiert verteilt.

⌘ Qualitätsabhängig:

- ⊠ Bis zu einer bestimmten Grenzfrequenz:
unverschlüsselter Broadcast
- ⊠ Anteile darüber: verschlüsselt

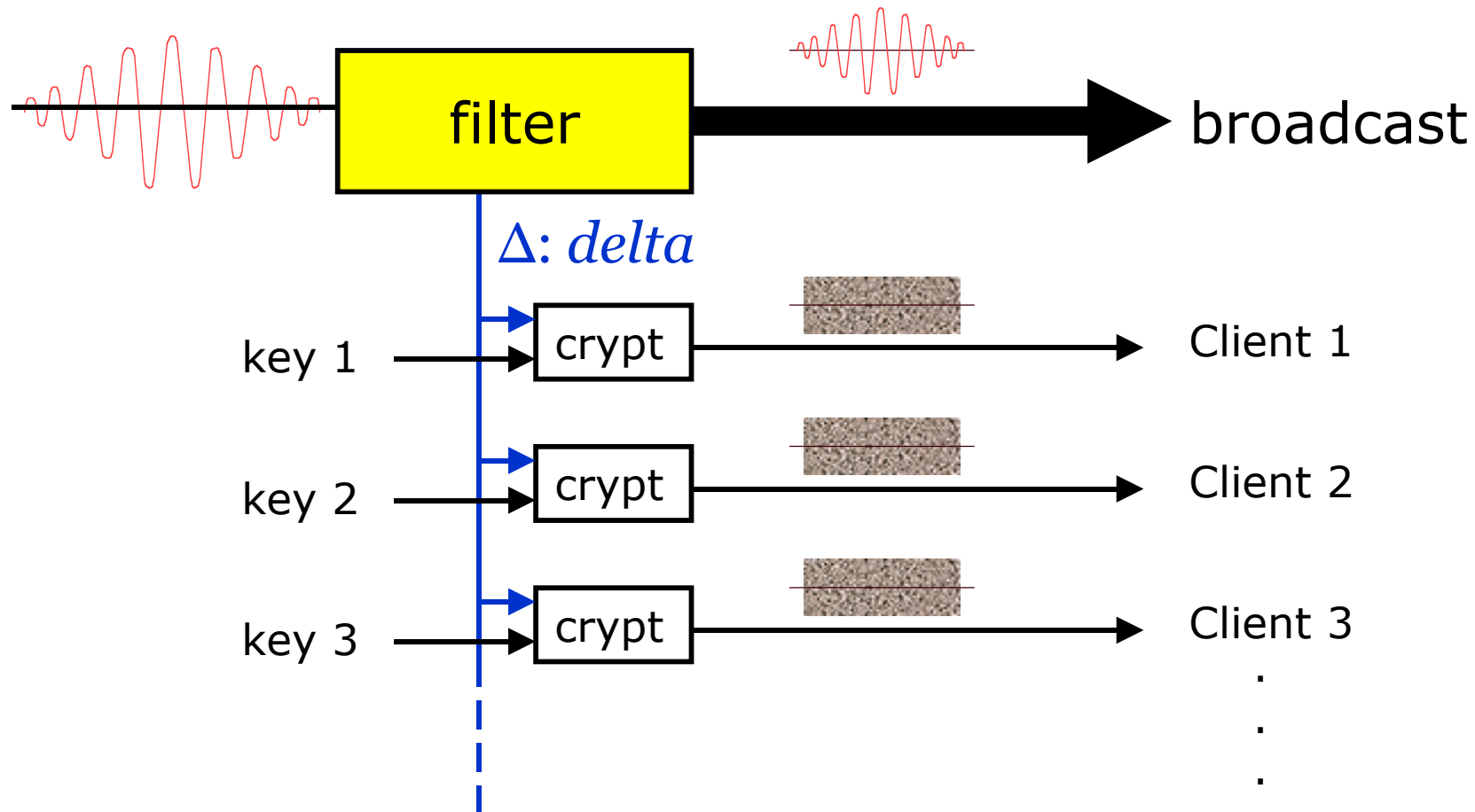
⌘ Stereo:

- ⊠ Summensignal Broadcast, Differenzsignal
verschlüsselt

⌘ MP3:

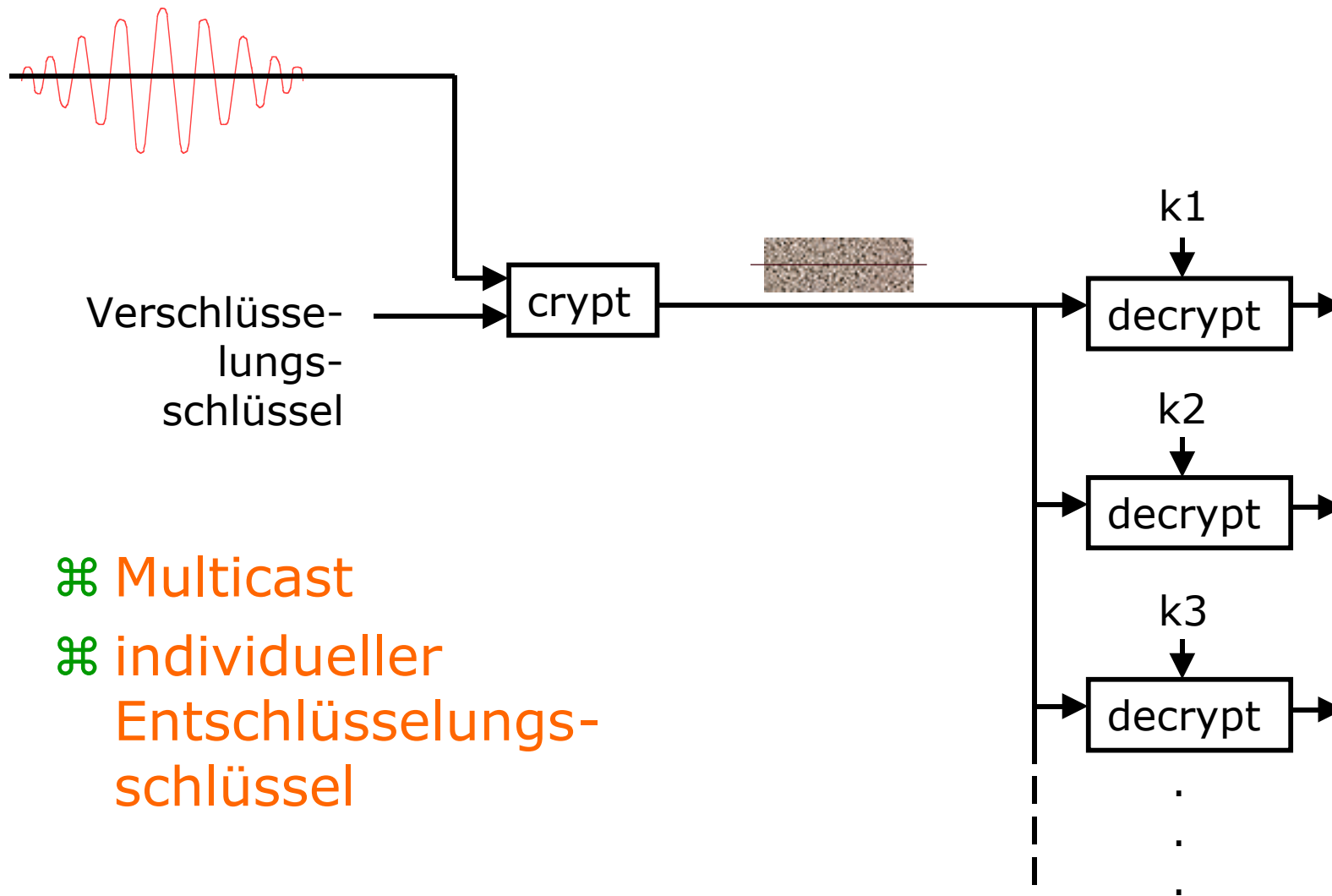
- ⊠ Aufteilung eines MP3 Stromes in Q-Stufen

> LoFi Broadcast, HiFi Encryption



⌘ Aufwand wächst linear mit Teilnehmerzahl

> Gruppenverschlüsselung

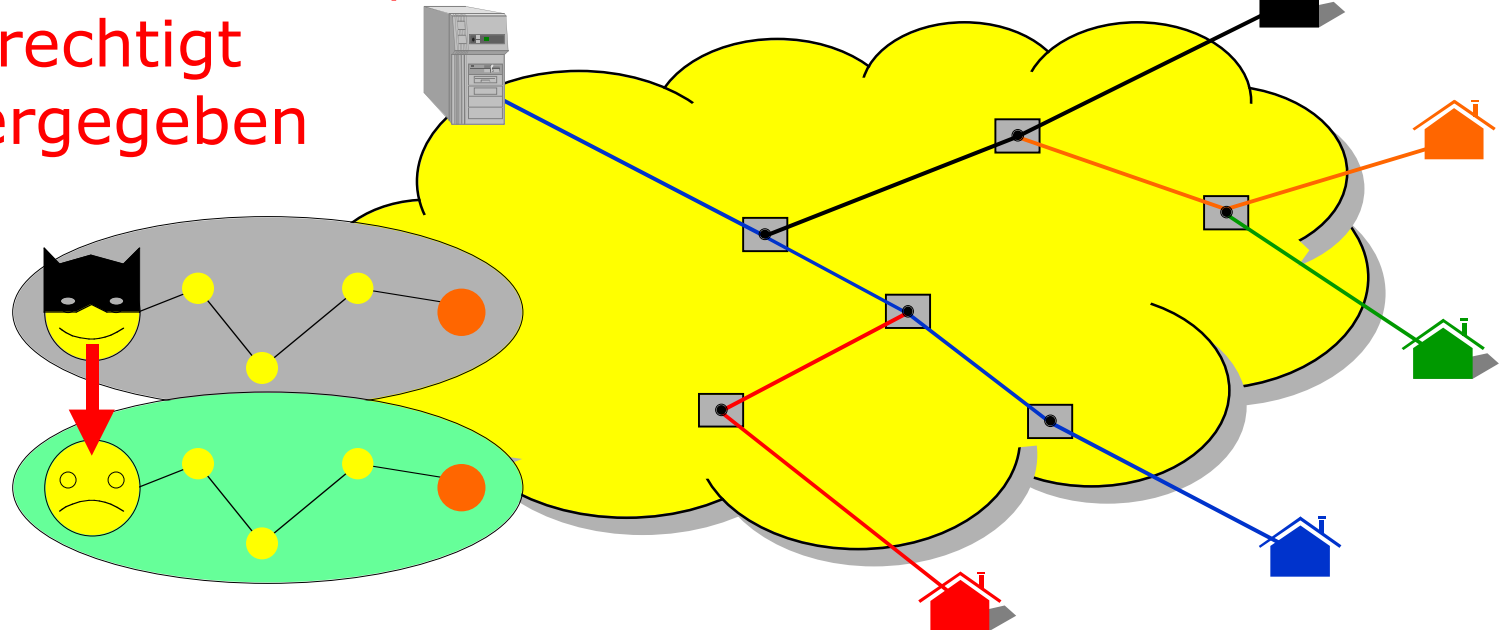


> Traitor Tracing

⌘ Fingerprinting

⌘ Broadcast Encryption

- ⊠ Ein Datenstrom für alle, aber *individueller Schlüssel*
- ⊠ Kombination mit Multicast
- ⊠ Es ist aufdeckbar, wer seinen Schlüssel unberechtigt weitergegeben hat



> Adressierung von Inhalten

- ⌘ Domain Name System (DNS)
- ⌘ Wer zuerst kommt... oder wem „gehört“ eine Domain-Adresse?
- ⌘ *Registrierung*: technischer Vorgang; Bedeutung von Entwicklern des Internet unterschätzt
 - ⊠ diene dem einfachen Merken von Adressen
 - ⊕ amadeus.icsi.berkeley.edu (128.32.201.196)
 - ⊠ ursprünglich nicht als Suchsystem entwickelt
- ⌘ Benutzer sollten *Suchmaschinen* verwenden, um an bestimmte Inhalte zu gelangen
- ⌘ Verhalten der Benutzer jedoch anders

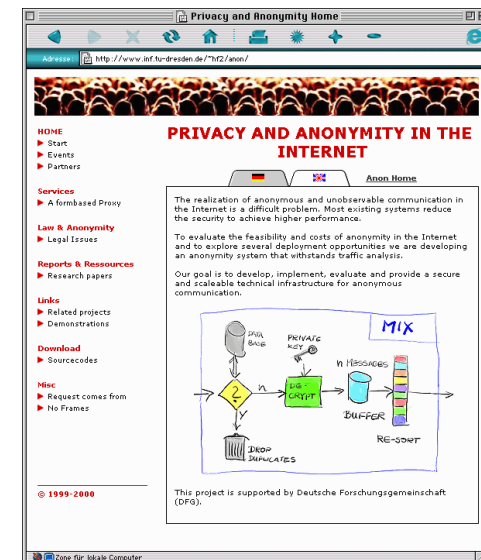
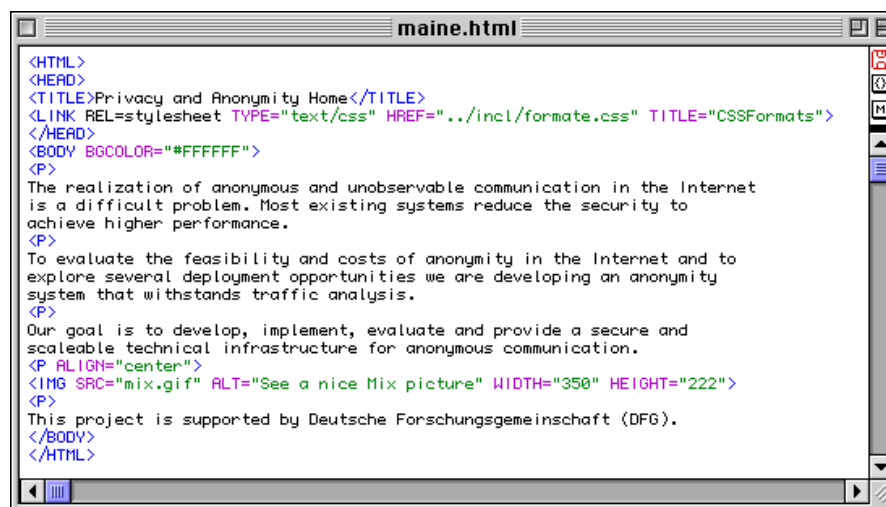
> Adressierung von Inhalten

⌘ Bzgl. des Regelungsbedarfs sollten 3 Ebenen unterschieden werden:

1. Domain-Namen (als Teil einer Adresse)
2. Begriffe in (Web)-Adressen

http://begriffe1-in-urls.**domain.com**/begriffe2-in-urls

3. Inhalte (Webseiten) selbst



> Filterung illegaler Inhalte

⌘ (MP3) Filter:

⊠ Filtern nach Adressen/Domains

- ⊕ Adressen können ständig gewechselt werden.
- ⊕ Gesamte Site muß gesperrt werden
- ⊕ Umgehung: Anon-Proxies/Redirector oder *ALLE* Internetknoten müssen filtern

⊠ Filtern nach Inhalten (on the fly, Bitmuster)

- ⊕ Umgehung durch Verschlüsselung

⌘ Nicht grundsätzlich wirkungslos, solange diejenigen, die nicht ernsthaft probieren, die Filterfunktion zu umgehen, die Zielgruppe sind.

- ⊠ Weitaus aufwendiger, Napster oder Gnutella zu programmieren, als entsprechenden Redirector

> Zusammenfassung

Hannes Federrath

<http://www.inf.tu-dresden.de/~hf2/>

⌘ Heute:

- ⊠ Peer-to-Peer Kommunikation
- ⊠ Verschlüsselung

⌘ Zukunft:

- ⊠ Multicast Protokolle
- ⊠ Watermarking
- ⊠ Traitor Tracing